REMARKS

Claims 1, 10, and 26-28 are pending.

Claims 1, 10, and 26-28 are rejected under 35 USC §103 as being unpatentable over the Monroe et al. U.S Patent No. 5,293,388 in view of Davis U.S Patent No. 5825,879 and Barnes et al. 4,172,213 (collectively, the cited documents). This rejection is respectfully traversed.

The present invention addresses the problem of sending ECC-encoded blocks to a computer bus that is not secure. In a DVD drive, for instance, it might be desirable to send certain ECC-encoded blocks from the drive to a host computer for ECC-decoding. The host computer could perform more flexible error correction methods than the drive. If, however, the blocks are sent to a bus that is to secure, the unencrypted data in the blocks would be vulnerable to theft and unauthorized copying.

The ECC blocks could be encrypted before being sent to the computer bus. However, the integrity of the code words would be destroyed by encryption such as RSA.

The applicant has found that a specific type of encryption – XOR encryption – does not destroy the integrity of the code words. The ECC blocks can be XOR-encrypted in the drive, and sent to a host computer for error code correction. Because XOR encryption is used, the host can perform the error code correction without having to decrypt the block. Error-corrected data, still encrypted, could then be sent downstream to an authorized device (e.g., an authorized DVD decoder card) for decryption. Thus, the host computer could perform the error code correction, yet still not have access to the encrypted data.

Claim 27 recites a drive comprising a reader; and a controller

programmed to perform a bitwise XOR of an encryption mask and a block of ECC-encoded data. A product of the bitwise XOR is an encrypted block. The controller is further programmed to output the encrypted ECC block.

None of the cited documents teach or suggest the desirability of performing XOR encryption on ECC blocks.

Figures 1-3 of Monroe et al. show a computer 10 including a host processor 80, a computer bus 20 that is connected to the computer 10, and a disk 30 that is connected to the bus 20 via an adapter 40. Figure 1 also shows a peripheral 50 (e.g., a backup tape drive) that is connected to the bus 20 via an adapter 60. The adapter 60 includes an ECC co-processor 65 and ECC RAM 66. The adapter sends compressed ECC data to the peripheral 50 (col. 1, lines 55-58).[1]

Monroe et al. do not teach or suggest encryption of the compressed ECC block. The office action acknowledges that Monroe et al. are silent about encryption of ECC blocks.

In Davis, Figure 1 shows a computer including a processor 104 and disk control subsystem 108 that are connected to a bus 128. Figure 1 also shows a video subsystem 116 connected to the bus 128. The video subsystem 116 includes a secure video content processor (SVCP) 132 for converting incoming digital content into an analog signal (see col. 2, lines 54-58)

1. For some reason, the office action asserts that the arguments in the previous response were based "on the fact that one particular example of a peripheral method by Monroe was a tape backup device." It is not known why the office action makes this assertion, or spends almost an entire page addressing it.

The SVCP 132 of Figure 1 corresponds to the SCVP 200 of Figure 2. The SCVP 200 includes decryption and decompression circuitry 228 that receives encrypted video content 212 from a video content source (e.g., CD ROM 220). According to Figure 5, encrypted digital video data is transmitted to the SVCP 200 (508), which decrypts the video data (512), processes the video data (514), re-encrypts the video data (516), and transmits the re-encrypted data to a memory unit.

Davis doesn't say much about the video source. The only passages appear to be located at col. 4, lines 27-31; and col. 6, lines 52-54. Neither of these passages mentions error code correction.

The office action states "It is inherent in Davis that means for handling compressed ECC data exist as the Thus it would have been obvious to one of ordinary skill in the art at the time the made, to have modified the invention of Monroe with the teaching of Davis to provide encrypted compressed data for displaying DVD which are high resolution (therefore ECC) high data density (compressed) and encrypted."

The inherency of handling ECC compressed data begs the issue. The issue is not whether Davis performs error code correction, but how, when and where the encryption is performed. Davis does not teach or suggest encrypting ECC-encoded data, let alone the choice of XOR encryption over the many different types of encryption.[2]

The office action confuses "high resolution" with error code correction. Resolution has to do with the number of bits describing a pixel of video. Error code correction has to do with the correction (and preservation) of data that might have been corrupted due to storage, transmission, etc.

2. Davis discloses RSA, DEA and DES encryption (col. 3, lines 1-12), which are much stronger than XOR encryption.

Barnes et al. disclose XOR encryption, but is silent about ECC coding. Thus, Barnes et al. provide no teaching, reason or suggestion to encrypt an ECC block with XOR encryption. At the end of paragraph 11 of the office action, a reason was given for using XOR encryption of ECC blocks ("Barnes use of the XOR cipher encryption would allow the error correction of Monroe to run in tack while maintaining the security ... required by Davis").[3] Unfortunately, the office action did not cite the document, column or line number where this reason could be found, and the undersigned did not find this reason in any of the cited documents. The examiner is respectfully requested to provide a pinpoint cite of this reason.

On paragraph 17 of the office action, the office action states that "Part of MPEG specification is error correction ECC." The relevance of this statement is not clear, as the office action does not explain. Further, it is assumed that this statement is within the personal knowledge of the examiner, since a document has not been cited (at col. 4, lines 51-55, Davis merely states that MPEG is used to compress and transmit moving images). The examiner is respectfully requested, pursuant to MPEP §707 and 37 CFR §1.104(d)(2), to provide an affidavit attesting to this personal knowledge about error correction with respect to the MPEG standard. The affidavit should specify how, when and where the error code correction is performed according to the MPEG standard.

To date, the office action provides no evidence of the desirability of performing XOR encryption of ECC blocks. Without any evidence to support the rejections, the office action provides little more than an unsubstantiated opinion. Because an unsubstantiated opinion does not provide a legal basis for claim rejections under U.S. patent laws, the '103 rejection of claim 27 should be withdrawn.

3. The remainder of the reason is not comprehensible and, therefore, is not being addressed.

Claim 28 recites a data controller comprising a processor for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data. A product of the bitwise XOR is an encrypted block.

As indicated above, the office action provides no evidence of the desirability of performing XOR encryption of ECC blocks, it only provides unsubstantiated opinions. Therefore, the '103 rejection of claim 28 should be withdrawn.

Claim 26 recites a system comprising a computer bus; a host processor programmed to perform error code correction; and a drive for providing an encryption mask, the drive performing a bitwise XOR of an encryption mask and a block of ECC-encoded data. A product of the bitwise XOR is an encrypted block. The drive provides the encrypted block to the computer bus, whereby an encrypted block can be sent to the host processor via the computer bus for error code correction.

The office action provides no evidence of the desirability of performing XOR encryption of ECC blocks, it only provides unsubstantiated opinions. For this reason alone, the '103 rejection of claim 26 should be withdrawn.

The '103 rejection of claim 26 should be withdrawn for the additional reasons that none of the cited documents teach or suggest a drive for providing an encryption mask, the drive performing a bitwise XOR of an encryption mask and a block of ECC-encoded data. Thus, the cited documents do not suggest all the claim limitations[4] of claim 26.

Claim 1 and its dependent claim 10 should be allowed over the cited documents for the same reasons that claim 26 should be allowed.

4. See MPEP §706.02(j)

An objection to the declaration has been noticed. The objection will be addressed following an indication of allowable subject matter.

The examiner is thanked for his suggestion concerning an amendment to figure 1. However, the amendment is viewed as unnecessary in view of the specification.

It is respectfully submitted that the present application is in condition for allowance. Reconsideration and allowance of the present application are earnestly solicited